Description

Method for detecting faults and supporting reconfiguration decisions in mobile-radio networks having reconfigurable terminals, and corresponding network elements and components

The invention relates to methods, network elements, and components for mobile-radio networks having reconfigurable terminals in which a new, hitherto unsupported radio technology is employed by replacing software that configures the terminal's transceiver.

Developing a new technology and using it in mobile telecommunication networks requires much effort in order to make sure the individual components will interact smoothly. That is conventionally achieved by means of costly standardizing - see for example GSM or UMTS - and by testing the individual components. That applies particularly to the network elements' interoperation with the terminals. However, a terminal's use of radio technologies is in the case present-day terminals restricted to a precisely defined possible range because using a radio technology means employing respectively special hardware for the respective radio technology. In contrast to this, in the case of reconfigurable terminals or, as the case may be, software-defined radio devices a software-programmable transceiver allows a new, hitherto unsupported radio technology to be used by replacing the software that configures the transceiver. New radio technologies and standards can therefore be used simply by downloading software onto the terminal, meaning that even existing terminals are able to use new technologies in the radio domain later.

The present UMTS standard for example places stringent demands on the terminals, resulting, inter alia, in some manufactur-

ers' already taking a "UMTS Lightweight" standard into consideration which, though less complex, nevertheless delivers the same performance in certain situations as the original standard. One of the associated prerequisites, though, is for not only the terminal but also the base station involved to be able to interpret the modified standard.

It is no longer guaranteed, though, through said new technology for terminals that interacting of the terminals such as, for instance, cell phones, with a base station or the other components in the network, can be fully tested. The terminals' reconfigurability can, even with utmost care being taken, give rise to disruptions resulting from software downloading. These can be due to faults in the applied software itself that can be ascribed to not being able to adequately test interacting with the network components for said devices.

The **object** of the invention is to disclose, on the one hand, a method for detecting faults and supporting reconfiguration decisions in mobile-radio networks having reconfigurable terminals and, on the other, corresponding network elements and agents by means of all of which greater reliability can be achieved in the interoperability of terminals and network elements in mobile-radio networks that support reconfigurable terminals.

Said object is achieved in method-related terms by means of the features of claim 1, in terms of the network element by means of the features of claim 6, and in agent-related terms by means of the features of claim 7. The further claims relate to preferred embodiments of the inventive method.

The invention relates essentially to a respective agent platform in network elements as well as to manufacturer-specific

agents installed on said platforms either directly or via agent providers' agent proxies, with said agents then receiving raw information about occurring operational faults via a defined interface of the agent platform and, together with manufacturer-specific information relating to the respective terminals or, as the case may be, types of terminal that is known only to the respective manufacturer, forming corresponding compressed decision information for evaluating fault incidents and/or optimizing reconfiguration decisions, and making said information available to the network element or, as the case may be, network operator and/or agent provider or, as the case may be, terminal manufacturer over the defined interface. That will result in greater reliability in the interoperability of terminals and network elements in mobile-radio networks having reconfigurable terminals.

The invention is explained in more detail below with the aid of exemplary embodiments shown in the drawing.

Figure 1 is a presentation for explaining a first exemplary embodiment of the invention, and

Figure 2 is a presentation for explaining a second exemplary embodiment of the invention.

Figure 1 shows agent-enabled network elements in a radio-access network, with one network element in the form of a radio-network controller, or RNC **RNCA**, being connected or, as the case may be, connectable to two terminals **T1A** and **T2A**, and a further network element in the form of a radio-network controller **RNCB** being connected or, as the case may be, connectable to three terminals **T1B**, **T2B**, and **T3B**, and being in each case supplied by agent providers **AP1**, **AP2**, and **AP3** directly or, as the case may be, immediately with agents **A1**, **A2**, and

A3. In this case the agent-enabled nodes are thus the RNCs of a UMTS. In other technologies these can be employed in network elements having an analogous function. For example in Wireless LAN (WLAN) networks, use in the WLAN access points will constitute an analogous use of said kind.

The agents exchange data directly with the respective agent provider, which is to say as a rule with the actual manufacturer or with a service provider. That, though, requires all the agents' application sites to be known directly to the agent provider. So the agent provider needs to know on which RNCs its agents have been installed.

Over defined interfaces of an agent platform of the network element the agents **A1**, **A2**, and **A3** receive raw information needed for evaluating fault incidents as well as for optimized decision-making in terms of terminal reconfiguring. Said information is processed or, as the case may be, compressed into decision information inside the component.

Figure 2 likewise shows agent-enabled network elements in a radio-access network which differ from those shown in figure 1 only in that the RNCs **RNCA** and **RNCB** are supplied with agents **A1**, **A2**, and **A3** not directly but via an agent proxy **APX** of the agent providers **AP1**, **AP2**, and **AP3**. An agent proxy **APX** mediates communication between the RNCs on which agents have been installed with their providers, with the agent proxy constituting a central location which the network elements access and which assumes the managing of which agent provider will supply the desired information. The providers **AP1**, **AP2**, and **AP3** can in their turn send requests and messages for their agents **A1**, **A2**, and **A3** directly to the agent proxy **APX**, which distributes the messages among the agents concerned. During installing or, as the case may be, uninstalling, the RNCs on which specific

manufacturers' agents have been installed are registered on the agent proxy **APX** so that the individual agents **A1**, **A2**, and **A3** on the RNCs **RNCA** and **RNCB** can be addressed via the proxy **APX**.

The network elements in mobile-radio networks, for example RNCs, are equipped with areas or, as the case may be, agent platforms for agents of said kind, with said platforms assuming, for instance, the allocating of computing time for the agents and the controlling thereof. The area in which the agents run is therein protected such that accessing is possible only by specially authorized users, which is to say by the manufacturer of the respective component. The agent platform is therein embodied such that the agent itself is conveyed encrypted so the software will not be accessible to third parties. The platform must furthermore authorize itself with the agent to insure that third parties will not be able to use the software. The transmission of data between the agent and respectively usage-authorized manufacturers, which is to say the agent providers, is safeguarded via just such measures so that the data being transmitted will be treated as confidential and can only reach the authorized manufacturer.

The network operator has control over who is able to employ agents on same's network elements, but has no, or only limited, access to the agent's data itself.

Moreover, the network element itself only grants the respectively authorized agent access to the data. That means agents can be produced securely, for example by the manufacturer of a specific type of terminal. Said agents can then perform functions on the network elements independently without third parties' being able to access the confidential information.

The invention's application is not, however, restricted solely to RNCs; it can further be applied to base transceiver stations (BTS). Through the use of agents, in addition to the exemplary applications cited hitherto it is possible there to realize manufacturer-specific expansions made to the respective mobile-radio standard. It is herein assumed that manufacturers of mobile-radio terminals will in the future employ their own manufacturer-specific expansions made to the mobile-radio standard in order to provide their devices with additional advantages. These can include reducing the data rate by using a narrower frequency band, as a result of which the mobile-radio cell's existing capacity can be better utilized because more terminals can share a band.

However, said non-standard-compliant terminals require a manufacturer-specific expansion of the functionality of the BTS because this has to support the expansions made to the standard. Said functionality can be made available by the terminal manufacturer by providing suitable agents for the BTS. Terminals of said type can as a result be used with any BTS equipped with an agent platform without the BTS manufacturer's having, when designing the BTS, to take account of such expansions made to the standard selectively for specific manufacturers. Neither will the terminal manufacturer have to disclose all details of same's manufacturer-specific expansion because these can be processed by the respectively associated agents on the BTS. The design of the interface of the agent platform having the BTS can furthermore insure that the manufacturer-specific expansions made to the standard will not conflict with the behavior of other mobile-radio users.

Analyzing faults and gathering fault data

Over defined interfaces of an agent platform the network elements therein makes information available to a manufacturer's

agent about faults occurring in connection with the relevant manufacturer's devices. Included here, for instance, are infringements of network protocols, infringements of the radio standard, for example if the terminal uses a frequency range other than that requested or violates time specifications, and other events resulting in network disruption.

However, information about said type of malfunctioning usually arises in the domain of the network operator who, though, not being in possession of the relevant device's full, generally not publicly accessible specifications, is unable to interpret said information adequately. Said information is, though, necessary if the network is to operate smoothly. Devices in particular that seriously impair network operation must be identified and, through appropriate measures, prevented from continuing to disrupt network operation. That can be done by, for example, selectively applying bug fixes to the terminal software. That, though, necessitates analyzing the operational data and communicating with the network elements. Conveying all data to the manufacturer would, however, entail an unreasonable amount of communication and include conveying sensitive data about mobile-radio users' behavior. The necessary procedure is, moreover, dependent on the type of terminal used and can be based on information the manufacturer does not wish to disclose.

The agent gathers relevant fault incidents and conveys data or, as the case may be, compressed information about them to the manufacturer. The faults can, moreover, also be analyzed by the agent and necessary decisions taken, for example reconfiguring the terminal into a failsafe default mode, initiating software downloading in order to replace faulty software with a later version, or disabling the terminal if an operationally safe condition cannot be attained. That is achieved using spe-

cial commands which the agent can send to the terminal. These are safeguarded by authorization codes such that misuse by third parties is precluded.

Support in the reconfiguration decision

Such information is, moreover, also needed for decisions/algorithms whose purpose is to take the best possible decision about changing over between radio technologies. It must therefore be provided in a manner allowing the operators of the networks to achieve best possible utilization of their networks without having to make the relevant information known publicly, in particular, though, to manufacturers of network elements (and of the software running thereon). Such information can relate to, inter alia, terminal characteristics such as the terminal's energy consumption in specific radio modes, the duration of reconfiguring, or the transceiver's precise characteristics.

The network element directs an inquiry to the respective manufacturer's agent, which it processes using the data accessible only to it as well as the information supplied as part of the inquiry by the network element. In response to the inquiry the agent sends the network element a recommendation that can be used to optimize the flows in the network. Configuration parameters of reconfigurable terminals as well as manufacturer-specific reconfiguration mechanisms are thus encapsulated within the agent. Neither the network operator, nor the user of the mobile terminal, nor other device manufacturers have access to said data.

Decisions about optimal reconfiguring are, as already indicated above, partially relocated to manufacturer-specific agents which, using the information made available to them and the manufacturer-specific data known only to them, produce de-

cision proposals which the RNC can take into account.

Advantages

Network elements that are agent-enabled such as, for example, RNCs, access points, and analogous devices, are able to support reconfigurable terminals such as, for instance, mobile telephones, Private Digital Assistants (PDAs), and notebooks significantly better than can network elements of conventional design.

The higher possible fault rate resulting from the flexible programming of the terminals' protocol stack can be better controlled by including manufacturer-specific algorithms/information. In particular, faults that occur can be better detected and interpreted because software provided by the device manufacturer can assume this function. This allows malfunctions to be correctly interpreted and suitable measures initiated such as, for example, disabling or, as the case may be, initiating reconfiguration to faultlessly operating default modes, or recognizing the need to update the software. Moreover, the system can serve to detect sources of faults in the terminal's software early by gathering information about the frequency of faults and their nature and making it available to the manufacturer.

A further improvement in reliability can also be achieved by providing manufacturer-specific fallback actions to be taken in the event of a fault which, despite the presence thereof, also allow normal operation to be continued without updating the terminal's software until a suitable software update is available for the terminal.

A further advantage of the invention is to be seen in the improved manner in which decisions about reconfiguring the ter-

minals can be taken. While deciding, the agents can take account of manufacturer's specifics without said details' having to be made known publicly. The technology employed furthermore allows said manufacturer-specific software components to be easily exchanged and replaced with a new one, which in turn allows account to be taken of changes to terminals as well as the introduction of new terminals.

The invention will furthermore allow expansions made to mobile-radio standards to be employed sooner. That means new manufacturer-specific expansions made to existing standards, which expansions can contribute to, for example, improved use of the resources in mobile-radio cells, can in a simple manner be employed in mobile-radio networks equipped with BTSs according to the present invention.